~~SECRET//SI//REL TO USA, FVEY~~

UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

USSID FA6001

(U) SECOND PARTY SIGINT RELATIONSHIPS

ISSUE DATE: 22 August 2012

REVISED DATE:

(U) OFFICE OF PRIMARY CONCERN

(U) National Security Agency/Central Security Service (NSA/CSS)
Foreign Affairs Directorate

(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION

(U) Topic of Promulgation	(U//~~FOUO~~) USSID FA6001 provides policy and guidance to elements of the United States SIGINT System (USSS) concerning relationships with Second Party SIGINT organizations. While USSID FA6101, "Third Party SIGINT Relationships," dated 31 October 2007, revised 29 September 2009, provides policy and guidance concerning other foreign relationships, NSA/CSS maintains a closer relationship with the SIGINT organizations in Australia, the United Kingdom, Canada and New Zealand by virtue of the British-U.S. Communications Intelligence Agreement (UKUSA), dated 5 March 1946.
(U) USSID Edition	(U) This USSID supersedes USSID FA6001, dated 22 March 1993, which must now be

~~SECRET//SI//REL TO USA, FVEY~~

destroyed.

(U) Legal Protection of Sensitive Information

(U//~~FOUO~~) This USSID contains sensitive information that is legally protected from release to any member of the public and is to be used only for official purposes of the NSA/CSS.

(U) Handling of USSID

(U) Users must strictly adhere to all classification and handling restrictions (see NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Manual," dated 23 November 2004, revised 8 January 2007) when:

- (U) storing hard or soft copies of this USSID, or
- (U) hyperlinking to this USSID.

(U) Users are responsible for the update and management of this USSID when it is stored locally.

(U) Location of Official USSID

(U//~~FOUO~~) The Chief, SIGINT Policy will maintain and update the current official USSID on NSANet (type "go ussid"). Selected USSIDs are also available on an access-controlled INTELINK Web page. Requests for access to the INTELINK USSID Page are granted based on mission need. (See the following INTELINK site: https://orcon.mall.nsa.ic.gov/producer/ussid/.)

(U) Access by Contractors and Consultants

(U) For NSA/CSS elements to include the SIGINT Extended Enterprise:

(U//~~FOUO~~) USSS contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT Extended Enterprise are pre-authorized for access to USSIDs via NSANet, INTELINK, or in hard-copy formats as needed to perform their jobs. However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.

(U) Outside NSA/CSS elements:

(U//~~FOUO~~) Non-USSS contractors or consultants working at external facilities are pre-authorized for soft-copy access to USSIDs via NSANet or INTELINK, if connectivity to those systems is allowed by the contractors' NSA/CSS sponsor. Where such connectivity is not established, any hard-copy provision of USSIDs must be authorized by the Chief, SIGINT Policy (NSA/CSS Secure Telephone System (NSTS): 966-5487, Secure Terminal Element (STE): (443) 479-1489, Defense

(b) (3)-P.L. 86-36

Switched Network (DSN): 689-5487).

(U) Access by Third Party Partners

(U) To request a shareable version:

- (U) Refer to USSID SP0002, Annex B; and
- (U) Contact the appropriate Country Desk Officer (CDO) in the NSA/CSS Foreign Affairs Directorate (DP).

(U) Executive Agent (U) The executive agent for this USSID is:

//S//
TERESA H. SHEA
Signals Intelligence Director

(U) TABLE OF CONTENTS

(U) Sections

(U) Annexes and Appendices

ANNEX A - (U) SIGINT LIAISON WITH AUSTRALIA, CANADA, NEW ZEALAND, AND THE UNITED KINGDOM

ANNEX B - (U) RELEASE OF U.S. SIGINT INFORMATION TO SECOND PARTY PARTNERS

SECTION 1 - (U) POLICY

(U) Policy

1.1. (U//~~FOUO~~) The SIGINT Director is committed to continuing foreign partner cooperation in mutually beneficial relationships, in accordance with U.S. laws and policy, including Director of National Intelligence (DNI) and Secretary of Defense (SECDEF) guidance. The Office of the Director of National Intelligence (ODNI) establishes policy governing procedures for the overall conduct of all SIGINT arrangements with foreign governments in accordance with DCID 5/5, "Conduct of SIGINT Liaison with Foreign Governments and the Release of U.S. SIGINT to Foreign Governments."

1.2. (U//~~FOUO~~) SIGINT relationships with foreign nations, to include close international partners Australia, Britain, Canada, and New Zealand, have in the past provided, and must continue to provide a clear benefit for the United States and, as specified in DCID 6/6, "Security Controls of the Dissemination of Intelligence Information," dated 11 July 2001, promote the interests of the United States, is consistent with U.S. law, and does not pose unreasonable risk to U.S. foreign policy or national defense. U.S. SIGINT technology, resources, and collection shared with foreign partners must also enhance U.S. national interests through contributions by the SIGINT partner, support U.S. strategy when SIGINT is to be shared, and contribute to U.S. defense and intelligence goals.

(U) Executive Agent

1.3. (U//~~FOUO~~) The Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) executes ODNI policy guidance in the conduct of SIGINT arrangements with Australia, Canada, New Zealand, and the United Kingdom (UK) (hereinafter referred to as Second Parties). The Second Party SIGINT organizations are the Defence Signals Directorate (DSD) for Australia, the Communications Security Establishment Canada (CSEC) for Canada, the Government Communications Security Bureau (GCSB) for New Zealand, and the Government Communications Headquarters (GCHQ) for the UK.

SECTION 2 - (U) RESPONSIBILITIES

(U) DIRNSA/CHCSS

2.1. (U//~~FOUO~~) DIRNSA/CHCSS, with the approval of the ODNI, appoints a Special United States Liaison Officer (SUSLO) for each Second Party SIGINT organization. Each SUSLO is responsible for SIGINT liaison and exchange with the applicable accredited Second Party SIGINT organization. The SUSLO represents the ODNI and DIRNSA/CHCSS in all SIGINT relationships with that Second Party, and, in so doing, executes National Intelligence Board (NIB) policy guidance.

2.2. (U//~~FOUO~~) The SUSLO facilitates direct exchange of information to ensure that NIB members obtain SIGINT information produced by the appropriate Second Party SIGINT organization. The SUSLO also assists in arranging meetings and exchanges of information between NIB members and their Second Party counterparts.

(U) NSA/CSS Organizations

2.3. (U//~~FOUO~~) The NSA/CSS Associate Directorate for Policy and Records (DJ) is responsible for the staff administration of the policies and procedures established in this USSID.

2.4. (U//~~FOUO~~) NSA/CSS Mission/Resource Authorities (MRAs) and Senior Functional Authorities (SFAs) are responsible for ensuring compliance with established policy concerning the release of SIGINT materials.

SECTION 3 - (U) GENERAL

(b) (3)-P.L. 86-36

(U) U.S. - Second Party Collaboration

3.1. (U//~~FOUO~~) U.S.-Second Party collaboration (including [redacted] planning for emergencies, wartime operations, and combined exercises; and defining and conducting needed SIGINT research) is arranged by DIRNSA/CHCSS and the Second Party involved.

3.2. (U//~~FOUO~~) SIGINT procedures, nomenclature, and terminology are coordinated with Second Parties, using liaison channels, to ensure standardization insofar as practicable.

(U) Access to U.S. SIGINT

3.3. (U//~~FOUO~~) To access U.S. SIGINT information, Second Party nationals must meet and comply with all U.S. legal, security, oversight, and training guidelines. Access by a Second Party national to U.S. SIGINT organizations or U.S. SIGINT information is permitted only when the individual's clearance and Communications Intelligence (COMINT) category and subcategory access authorization have been certified, using liaison channels, and the request for access has been approved by the individual's parent organization. NSA/CSS is the final approving authority for Second Party access in accordance with Signals Intelligence Directorate (SID) Management Directive (SMD) 427, "Access to Data for Second Party Personnel Engaged in SIGINT Production," dated

1 August 2009.

SECTION 4 - (U) TECHNICAL EXCHANGE AND VISITS

(U) Technical SIGINT Material Exchange

4.1. (U//~~FOUO~~) Technical SIGINT is exchanged between U.S. and Second Party centers or field units in accordance with the provisions of USSID AP2402, "Technical Electronic Intelligence (ELINT) Signals Analysis, and Data Forwarding Procedures," dated 23 April 2001, and the forwarding instructions in the sites' respective unit USSID.

4.2. (U//~~FOUO~~)

(U) Visits and Engagements

4.3. (U//~~FOUO~~) Proliferation and availability of secure communications technology provides numerous opportunities to convey and exchange information that were previously unavailable. While in-person visits are important, USSS personnel will be increasingly encouraged to explore other means to convey and exchange information. When a visit is necessary, approval is based on the following criteria.

a. (U//~~FOUO~~) The visit fulfills a requirement that cannot be satisfied through other established liaison channels.

b. (U//~~FOUO~~) The size of the visiting party and duration of the visit are consistent with the stated purpose of the visit and can be accommodated by the host facility.

c. (U//~~FOUO~~) The dates of the visit are convenient to the host facility.

(b)(3)-P.L. 86-36

d. (U//~~FOUO~~) The visit is mutually beneficial.

4.4. (U//~~FOUO~~) Visits between USSS elements (national to tactical) and Second Parties must be arranged in accordance with the guidelines established below. The affiliation of the visitor AND the organization to be visited determine which procedures should be followed:

4.5. (U) Second Party personnel visiting U.S. SIGINT organizations:

a. (U//~~FOUO~~) The visitor must propose the visit through the national SIGINT authority (GCHQ, CSEC, DSD or GCSB);

b. (U//~~FOUO~~) The national SIGINT authority will forward the visit proposal and

[redacted]

EXCEPTION 1: (U//~~FOUO~~) Intratheater visits should be processed locally (for example, SUSLOL handles proposed UK visits to U.S. SIGINT facilities in Europe; SUSLOC and SUSLOW respectively handle proposed Australian and New Zealand personnel visits to U.S. SIGINT facilities in the Pacific).

EXCEPTION 2: (U//~~FOUO~~) For visits to the Cryptologic Centers - The national SIGINT authority will forward the visit proposal and clearance certification to their [redacted]

4.6. (U) NSA/CSS personnel visiting Second Party facilities:

a. (U) Visits to Second Party facilities within Second Party national borders:

- (U) The visitor should forward visit proposal and clearance certification message to:
  - (U//~~FOUO~~) Special United States Liaison Officer, London (SUSLOL) and SUSLOL, Cheltenham (SUSLOL CHELT) for visits to the UK;
  - (U//~~FOUO~~) Special United States Liaison Officer, Ottawa (SUSLOO) for visits to Canada;
  - (U//~~FOUO~~) Special United States Liaison Officer, Canberra (SUSLOC) for visits to Australia; and
  - (U//~~FOUO~~) Special United States Liaison Officer, Wellington (SUSLO) for visits to New Zealand.
- (U//~~FOUO~~) DP should be included on distribution for all such visit proposals, but is no longer required to show concurrence on each of these messages;
- (U//~~FOUO~~) The appropriate theater NSA/CSS Representative (NCR) should be on distribution for all such visit proposals;
- (U//~~FOUO~~) [redacted]
- (U//~~FOUO~~) The SUSLO will coordinate with Second Party Partners for these visits.

(b) (3)-P.L. 86-36

b. (U//~~FOUO~~) Visits to Second Party facilities based outside the Second Party national borders:

- (U//~~FOUO~~) The visitor should contact the appropriate Second Party country CDO in DP for guidance early in the trip planning process.

4.7. (U//~~FOUO~~) U.S. service cryptologic personnel visiting in-theater Second Party SIGINT facilities:

(b) (3) -P.L. 86-36

a. (U//~~FOUO~~)

- (U//~~FOUO~~) DIRNSA/CHCSS or appropriate theater NCR must approve visits involving policy issues.

4.8. (U//~~FOUO~~) Other U.S. government personnel visiting Second Party SIGINT facilities:

a. (U//~~FOUO~~) Visits to Second Party SIGINT organizations:

- (U//~~FOUO~~) The visitor must propose the visit and forward the clearance to DP, who will coordinate within NSA/CSS and forward the proposal to the proper SUSLO; and

EXCEPTION: (U//~~FOUO~~) Intratheater visits should be processed locally. For example, United States European Command (USEUCOM) visits to UK SIGINT facilities should be proposed directly to SUSLOL; United States Pacific Command (USPACOM) visits to Australia or New Zealand SIGINT facilities should be proposed directly to SUSLOC and SUSLOW respectively.

- (U//~~FOUO~~) All visit proposals must be formally approved by the Second Party partner; the forwarding of clearances does not constitute visit approval. DP or SUSLO will notify visitors of approval when received from the Second Party.

b. (U//~~FOUO~~) Visits to Second Party government facilities if special intelligence certification is required:

- (U//~~FOUO~~) If the visit is to a military facility, visitor should forward a visit proposal and clearance certification message directly to the Staff Security Officer (SSO) of the Second Party military center as follows:
  - (U//~~FOUO~~) For visits to UK military facilities, send a message to British

(b) (3) -P.L. 86-36

  - (U//~~FOUO~~) For visits to Canadian military facilities, send a message to

[redacted]

- (U//~~FOUO~~) For visits to Australian military facilities, send a message to [redacted]
- (U//~~FOUO~~) For visits to New Zealand military facilities, send a message [redacted]

- (U//~~FOUO~~) If the visit is to a nonmilitary facility, the visitor should forward a visit proposal and clearance certification message as follows:
  - (U//~~FOUO~~) For visits to UK nonmilitary facilities, send a message to SUSLOL CHELT//SSO// with an information copy to "SUSLOL";
  - (U//~~FOUO~~) For visits to Canadian nonmilitary facilities, send a message to SUSLOO;
  - (U//~~FOUO~~) For visits to Australian nonmilitary facilities, send a message to SUSLOC; and
  - (U//~~FOUO~~) For visits to New Zealand nonmilitary facilities, send a message to SUSLOW.

(b) (3)-P.L. 86-36

4.9. (U//~~FOUO~~) U.S. contractors visiting Second Party SIGINT facilities for SI-level discussions:

a. (U//~~FOUO~~) The contractor must have an NSA/CSS sponsor.

- (U//~~FOUO~~) If the contractor is working directly with a Second Party SIGINT organization and does not have an NSA/CSS sponsor, DP will fulfill the NSA/CSS sponsor role;
- (U//~~FOUO~~) The NSA/CSS sponsor is responsible for verifying clearances and forwarding the visit proposal and clearance certification message to the appropriate SUSLO; and
- (U//~~FOUO~~) Include the NSA/CSS Office of Industrial and Acquisition Security (Q13) on distribution for all contractor clearance messages.

4.10. (U//~~FOUO~~) Second Party cryptologic personnel and their contracting representatives visiting U.S. contractor facilities for SI-level discussions:

a. (U//~~FOUO~~) [redacted]

b. (U//~~FOUO~~) DP will conduct any coordination required for the visit;

c. (U//~~FOUO~~) The NSA/CSS sponsoring organization must complete the Clearance Certification Form (form G2901) and forward it to DP for signature; and

- (U//~~FOUO~~) If NSA/CSS is not sponsoring the visit, the appropriate liaison office must complete form G2901 and forward it to DP for signature.

d. (U//~~FOUO~~) DP will sign the form and forward it to the NSA/CSS Special Access Office (Q23).

(U//~~FOUO~~) Visit Proposal Messages

4.11. (U//~~FOUO~~) All visit proposal messages must be forwarded [redacted] and contain the following visitor information:

(b)(3)-P.L. 86-36

[redacted]

SECTION 5 - (U) COMBINED PARTIES AND INTEGRATED PERSONNEL ASSIGNMENTS

(U) SIGINT Agreements

5.1. (U//~~FOUO~~) Agreements between DIRNSA/CHCSS and Second Party SIGINT directors provide for the establishment of combined operational and research efforts and integrated personnel assignments at SIGINT locations.

(U) Second Party Integration

5.2. (U//~~FOUO~~) In accordance with NSA/CSS Policy 1-13, "Second Party Integrees," dated 29 December 2010, the integration of Second Party personnel into USSS sites will

be supported when it is beneficial to the U.S. SIGINT or mission. The establishment of these positions must be coordinated with, and approved by DP prior to staffing more fully within NSA/CSS.

(U) Security Ramifications

5.3. (U//~~FOUO~~) Security ramifications ( ) associated with Second Party integrees must be considered prior to establishing and staffing any positions. In accordance with NSA/CSS Policy 1-13 and SMD 427, Second Party integrees should not be placed in positions where they might influence or represent the U.S. SIGINT decision-making process, including both contractual and policy deliberations.

(b) (3)-P.L. 86-36

SECTION 6 - (U) SECURITY AND CLASSIFICATION

(U) SIGINT Security Procedures

6.1. (U//~~FOUO~~) SIGINT security procedures and criteria are mutually agreed to by U.S. and Second Party policy authorities and are contained in USSID SP0003.

(U) Classification

6.2. (U//~~FOUO~~) As of December 1983, the fact that DIRNSA/CHCSS has a relationship with any or all Second Party countries, or that they exchange liaison officers and conduct liaison concerning SIGINT, is unclassified.

(b) (3)-P.L. 86-36

SECTION 7 - (U) SECOND PARTY SIGINT ORGANIZATIONS AND LIAISON OFFICES

(U) Second Party SIGINT Organizations

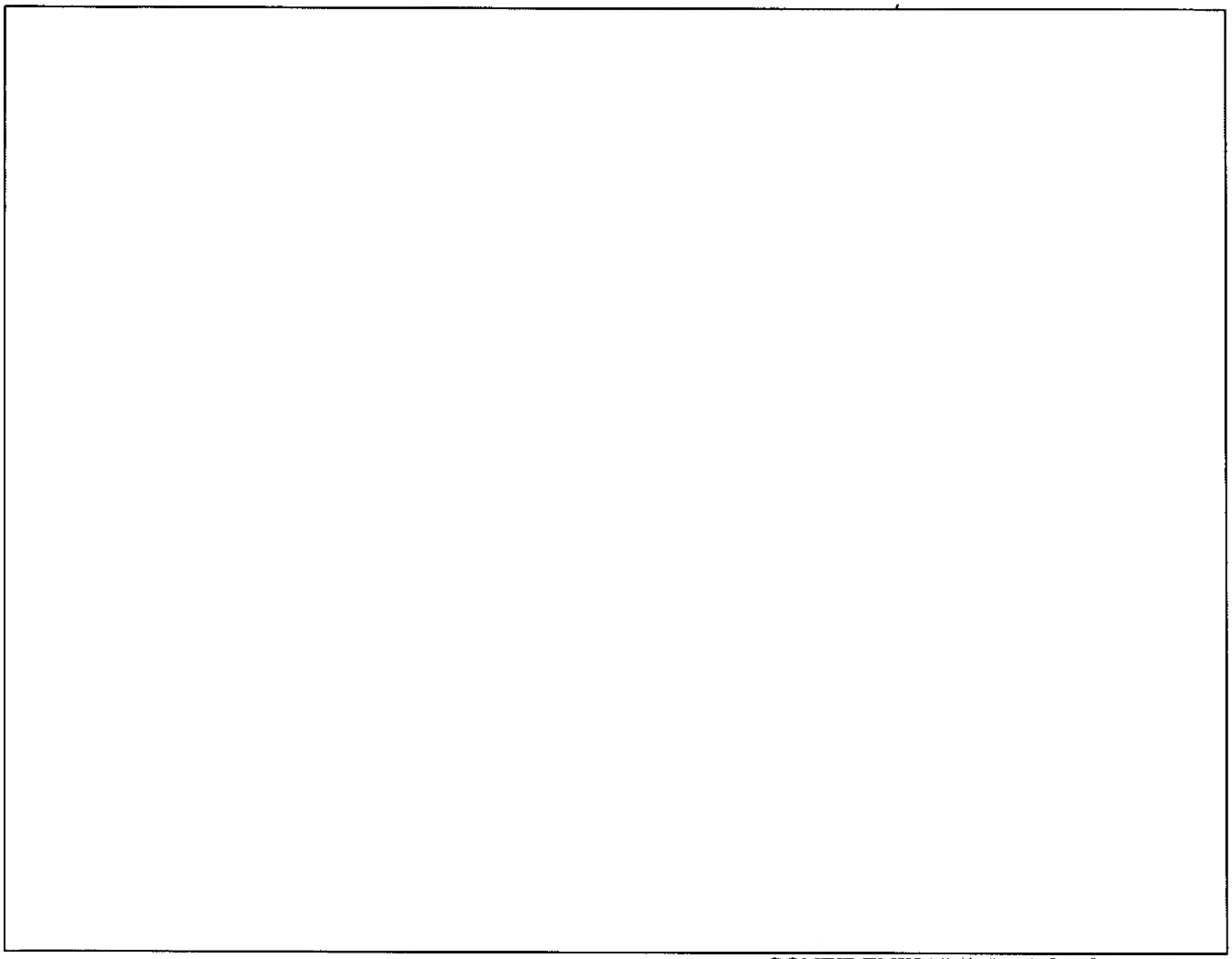
7.1. (U//~~FOUO~~) The Second Party locations and liaison offices, and NSA/CSS liaison offices associated with Second Parties, that appear in NSA/CSS correspondence are:

~~CONFIDENTIAL//REL TO USA, FVEY~~

Second Party SIGINT Organizations

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36



USSID FA6001
ANNEX A - (U) SIGINT LIAISON WITH AUSTRALIA, CANADA, NEW ZEALAND, AND THE UNITED KINGDOM

SECTION 1 - (U) PURPOSE

(U) Purpose A1.1. (U) This Annex delineates procedures and responsibilities for conducting SIGINT

liaison with Second Party collaborating centers.

SECTION 2 - (U) RESPONSIBILITIES

(U) SUSLO

A2.1. (U) The SUSLO, as the senior representative of DIRNSA/CHCSS to the Second Party organization, is responsible for ensuring the continued effectiveness of SIGINT collaboration.

(U) The Associate Directorate for Policy and Records

A2.2. (U//~~FOUO~~) DJ is responsible for the conduct of policy for DIRNSA/CHCSS. SID, the Information Assurance Directorate (IAD), and DP are responsible for the conduct of foreign relations planning.

(U) Director of Foreign Affairs

A2.3. (U//~~FOUO~~) The Director, Foreign Affairs is the principal agent of DIRNSA/CHCSS for supervising the conduct of liaison with foreign partners. Within DP, DP1 (SIGINT Operations) is responsible for Second Party SIGINT relations, and DP2 is responsible for Second Party Information Assurance relations.

(U) Commanders of the U.S. Service Cryptologic Components (SCCs)

A2.4. (U//~~FOUO~~) The commanders of U.S. SCCs, and their respective service representatives, are authorized to conduct liaison with respective in-theater Second Party military colleagues on SIGINT matters relating to the interoperability of military tactical systems, SIGINT operational capabilities, tactics, training, personnel utilization, etc. This includes exchange visits between cryptologic personnel attached to military units and other non-SIGINT organizations.

(b) (1)
(b) (3)-P.L. 86-36

a. ~~(S//SI//REL)~~ Prior approval for liaison on non-routine SIGINT matters must be obtained by the SCC from DIRNSA/CHCSS. Respective SCC Headquarters and the appropriate SUSLO must be included on correspondence requesting such approval.

b. (U//~~FOUO~~) SCC subordinate elements must report any significant actions taken, agreements made, or subjects discussed during such liaison to DIRNSA/CHCSS, the respective SCC Headquarters, DP, and the appropriate SUSLO.

SECTION 3 - (U) PROCEDURES

(U) General

A3.1. (U//~~FOUO~~) Effective SIGINT liaison between DIRNSA/CHCSS and Second Party Partners requires the use of SUSLOs as the channels to Second Party Partners. Similarly, Second Party Partner liaison officers are channels to liaison with NSA/CSS.

A3.2. (U//~~FOUO~~) NSA/CSS Headquarters elements use "DIRNSA" (vice NSA) as the "FROM" addressee when corresponding with SUSLOs or Second Party centers.

A3.3. (U//~~FOUO~~) For administrative-related matters (Temporary Duty (TDY), personnel actions, etc.), do not include either the Second Party HQ or its liaison office at NSA/CSS as an action or information addressee.

A3.4. (U//~~FOUO~~) Information Assurance inquiries should be forwarded to the Information Assurance Directorate (IAD) with information copies to DP's SIGINT Operations Group (DP1) and Information Operations Group (DP2). Since this is a USSID (SIGINT Directive), it is NSA/CSS FAD's recommendation that the information on IA be limited to what has been proposed. IAD documentation should address foreign partner engagement.

(U) Second Party Liaison and Collaboration

A3.5. (U//~~FOUO~~) The SUSLOs include the SUSLOC (Canberra), the SUSLOO (Ottawa), the SUSLOW (Wellington), and the SUSLOL (London). Each SUSLO must be kept informed of developments that pertain to, or may affect, NSA/CSS and Second Party relationships.

A3.6. (U//~~FOUO~~) DSD, CSEC, GCSB and GCHQ have established

(b) (3) -P.L. 86-36

a. (U//~~FOUO~~) If it is necessary to consult these offices before approaching the SUSLO, advise the SUSLO as soon as possible thereafter. Whenever substantive information is passed orally to a liaison officer, prepare a brief Memorandum for the Record of the conversation, and forward copies to the SUSLO, DIRNSA/CHCSS, DP1, and DP2 for IA, by the most expeditious means.

b. (U//~~FOUO~~) Send to the concerned Second Party liaison office all replies to queries or actions from that office, even if the correspondence responds to a communication that has been forwarded from the director or chief of a Second Party HQ. Such correspondence must be coordinated with DP prior to release. Furnish information copies to the SUSLOs concerned.

USSID FA6001
ANNEX B - (U) RELEASE OF U.S. SIGINT INFORMATION TO SECOND PARTY SIGINT ORGANIZATIONS

SECTION 1 - (U) PURPOSE

(U) Purpose

B1.1. (U//~~FOUO~~) This Annex sets forth the procedures for releasing U.S. SIGINT information to the Second Party SIGINT organizations.

SECTION 2 - (U) GENERAL

(U) Second Party Collaboration

B2.1. (U//~~FOUO~~) NSA/CSS and the Second Party Partners collaborate on a wide range of targets. The specific targets and degree of collaboration may change from time to time by mutual agreement and should be documented by a Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) or a Division of Effort (DOE) statement. Copies of all MOU/MOAs must be provided to the NSA/CSS Office of Corporate Policy (DJ), DP and SID SIGINT Policy. If a DOE Statement between NSA/CSS and Second Party elements is used to document efforts against similar targets, a copy of this statement must be provided to DP1.

(U) SIGINT Material

B2.2. ~~(S//SI//REL)~~ Second Party Partners receive raw traffic, technical material, and serialized SIGINT reports derived from the U.S. effort on mutual targets, in accordance with U.S. government policy and guidelines to include SMD 427, as applicable.

(U) Intelligence Information Requirements

B2.3. ~~(S//SI//REL)~~ Second Party Partners require intelligence information on issues impacting international relations, and on events related to the partners' political, economic, military, or security interests. However, no U.S. SIGINT information will be used or disseminated by Second Party Partners in a way that contradicts U.S. government policy and national security goals and objectives or is inconsistent with U.S. law. In addition to serialized reports furnished to Second Party Partners to meet the specific intelligence requirements, consideration must also be given to:

a. ~~(S//SI//REL)~~ [redacted]

b. ~~(S//SI//REL)~~ [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

c. ~~(S//SI//REL)~~

SECTION 3 - (U) RESPONSIBILITIES

(U) NSA/CSS Senior Management

B3.1. (U//~~FOUO~~) NSA/CSS Deputy Directors/Associate Directors/Chiefs are responsible for ensuring compliance with established procedures when releasing SIGINT material under their purview to Second Party Partners. They are also responsible for providing any attendant technical support.

(U) Information Sharing Services

B3.2. (U//~~FOUO~~) NSA/CSS SID Information Sharing Services (S12) maintains records of serialized reports, including field-produced serialized reports, that are released to Second Party Partners. Proposed distribution changes must be coordinated with S12 and DP1. S12 will review SIGINT exchanges with Second Party Partners that also involve distribution to a third nation, such as in combined exercises.

SECTION 4 - (U) PROCEDURES

(U) Release of SIGINT Material

B4.1. (U//~~FOUO~~) SIGINT material relevant to the requirements of a Second Party Partner is directly forwarded to the partner location.

B4.2. (U//~~FOUO~~) Release of new categories or types of SIGINT material is to be coordinated with DP1 and S12.

B4.3. (U//~~FOUO~~) If U.S. SIGINT materials are required by a particular Second Party Partner, but cannot be released because of restrictions imposed by the producing, procuring, or supplying agency, S12 will review the need and coordinate with DP1.

Proceed To:
NSA | Director | SID | SID Staff | SID Policy | USSID Index